

1

ON-LINE VALUE-BEARING INDICIUM PRINTING USING DSA

CROSS-REFERENCE TO RELATED APPLICATIONS

5

This application claims the benefit of U.S. Provisional Application No. 60/183,927 filed February 22, 2000, and U.S. Provisional Application No. 60/182,935 filed February 16, 2000, which are hereby incorporated by reference as if set forth in full herein.

10

FIELD OF THE INVENTION

15

The present invention relates to generating value-bearing indicia such as postage or ticket indicia. More specifically, the invention relates to an on-line system for validating and printing value-bearing indicia in a Wide Area Network (WAN) environment.

20

BACKGROUND OF THE INVENTION

25

Value-bearing indicia (VBI) are used in a variety of transactions where a holder of a VBI is entitled to receive goods or services. The holder of the VBI surrenders the VBI in exchange for receiving the goods or services. Typical examples of transactions using VBI are using postage stamps to mail packages, using a ticket to gain access to board an airplane, and using traveler's checks to pay for goods and services.

30

Transactions involving VBI comprise at least two steps, a user purchases a VBI from an issuing entity such as a postage vendor or airline and then the user redeems the VBI at the time the user wants to take delivery of an item from the issuing entity or use a service provided by the issuing entity. Purchasing the VBI may require a secure method allowing the user to purchase a valid VBI from the issuing entity.

35

An example of purchasing a VBI from an issuing entity is the purchase of metered postage from the a postage vendor. A significant percentage of the United States Postal Service (USPS)

1 revenue is from metered postage. Metered postage is generated
by utilizing postage meters that print special marks, also known
as postal indicia, on mail pieces. Generally, printing postage
5 can be carried out by using mechanical postage meters or
computer-based systems.

With respect to computer-based postage processing systems,
the USPS under the Information-Based Indicia Program (IBIP) has
published specifications for IBIP postage meters that identify
10 a special purpose hardware device, known as a Postal Security
Device (PSD) that is generally located at a user's site. The
PSD, in conjunction with the user's personal computer and
printer, may function as the IBIP postage meter. The USPS has
published a number of documents describing the PSD
15 specifications, the indicia specifications and other related and
relevant information.

A significant drawback of existing hardware-based systems
is that a new PSD must be locally provided to each new user,
which involves significant cost. Furthermore, if the additional
PSD breaks down, service calls must be made to the user location.
20 In light of the drawbacks in hardware-based postage metering
systems, a software-based system has been developed that does not
require specialized hardware for each user. The software-based
system meets the IBIP specifications for a PSD, using a
centralized server-based implementation of PSDs and includes a
25 database for all users' information. The software-based system,
however, has brought about new challenges.

The software-based system should be able to handle secure
communications between users and the database. In a hardware-
30 based system, security is generally handled by the local hardware
piece, that is unique to each user and includes a cryptographic
module that encrypts that user's information.

Another example of purchasing a VBI from an issuing entity
is the purchase of a ticket to access a service such as an
35 airline flight. Typically, a user buys a ticket directly from

1 an airline or indirectly through a ticketing agency. The user
specifies a flight and the airline or ticketing agency generates
the ticket. The ticket generation process reserves a seat for
5 the user and creates a ticket that is given to the user.

A significant drawback of existing ticketing systems is that
the user may need to take physical possession of the ticket
before it can be used. Physical receipt of the ticket usually
requires that the airline or ticket agency mail the ticket to the
10 user. Alternatively, the user may accept receipt of the ticket
at a location prior to redeeming the ticket when boarding the
specified flight.

Therefore, a software based on-line ticketing system is
needed that is capable of issuing a ticket directly to the user
so that the user can print the ticket for themselves.
15 Furthermore, the issued ticket must be capable of being validated
when the user redeems the ticket.

SUMMARY OF THE INVENTION

20 According to the present invention, Value Bearing Indici-
(VBI) are generated for on-line applications using a digital
signature algorithm. A VBI is generated by hashing user
information to create a message digest that is used to create a
digital signature. The digital signature is combined with the
25 user information to create a VBI that can be validated by a
variety of stand-alone or on-line methods.

In one aspect of the invention, a user provides information
to an indicium generator server for generation of VBI. Relevant
information is received from the user via the computer network.
30 The relevant information is used to verify the identity of the
user. A message digest is generated by hashing a first subset
of the relevant information and a digital signature is generated
from the message digest. A 2-D bar code is generated from a
second subset of the relevant information and transmitted with
35

1 the digital signature via the computer network to the user to be printed as a value bearing indicia.

5 In another aspect of the invention, a data processing system is adapted to provide postage for a mail piece to a user via a computer network. The data processing system receives a set of postage information from the user via the computer network. The data processing system verifies authenticity of the user based on the postage information. The data processing system generates a message digest by hashing a first subset of the postage information and generates a digital signature from the message digest. The data processing system generates a 2-D bar code from a second subset of the postage information and transmits via the computer network the digital signature and the 2-D bar code to the user to be printed next to each other as postage for the mail piece.

BRIEF DESCRIPTION OF THE DRAWINGS

20 These and other features, aspects, and advantages of the present invention will become better understood with regard to the following description, appended claims, and accompanying drawings where:

FIG. 1 is a schematic of an exemplary client/server system for generating value bearing indicia;

25 FIG. 2 is a schematic of an exemplary general purpose computer adapted for use in a client/server system for generating value bearing indicia;

30 FIG. 3 is data process diagram of an exemplary process for generating a value bearing indicia using a digital signature algorithm;

FIG. 4 is an exemplary table of relevant data;

FIG. 5 is an exemplary hash table of data taken from the table of relevant data;

FIG. 6 is a second exemplary table of relevant data;

1 FIGS. 7A-7B are depictions of exemplary value bearing indicia;

5 FIG. 8 is a software architecture diagram of an exemplary postage system employing a value bearing indicium;

 FIG. 9 is a deployment diagram of an exemplary ticketing system employing a value bearing indicium according to the present invention;

10 FIG. 10 is a collaboration diagram depicting an exemplary ticket buying process using an exemplary ticketing system employing a value bearing indicium according to the present invention; and

15 FIG. 11 is a collaboration diagram depicting an exemplary ticket redemption process using an exemplary ticketing system employing a value bearing indicium according to the present invention.

20 DETAILED DESCRIPTION OF THE INVENTION

25 In one embodiment of the invention, an on-line value-bearing indicia printing system is based on a client/server architecture. Generally, in a system based on client/server architecture the server system delivers information to the client system. That is, the client system requests the services of a generally larger computer. In one embodiment, the client is a local personal computer and the server is a more powerful group of computers that house the information. The connection from the client to the server is made via a Local Area Network, a phone line or a TCP/IP based WAN on the Internet. Other forms of connections, such as wireless connection are possible. A primary reason to set up a client/server network is to allow many clients access to the same applications and files stored on the server system.

30 In one postage metering embodiment, the server system is remotely located in a separate location from the client. The server system is operably coupled to the client via the Internet. FIG. 1 illustrates a remote client system 220a connected to a

35

1 server system 180 via the Internet 221. The client system
includes a processor unit 223, a monitor 230, printer port 106,
a mouse 225, a printer 235, and a keyboard 224. Server system
5 180 includes Postage servers 132, Database 130, and cryptographic
modules 134.

10 In operation, a user uses the client system to transmit
relevant information 112 to the server system. The server system
generates a VBI 114 using a subset of the relevant information
and transmits the VBI to the client system. The client system
transmits the VBI 116 to the printer for printing. The user now
has a hard copy of the VBI printed by the client system. The
user takes the VBI and exchanges it for goods or services at
another location.

15 A client software in association with a server software
provides a graphical user interface (GUI) for interfacing with
users and processing the information entered by the user. When
a user activates a "print" button in a dialog box within the GUI,
information such as the amount of the item or postage and other
relevant data are transferred to the server. The PSD within a
20 cryptographic device then generates a unique digital signature
(discussed in more detail below) for the digital signature field
of a postage indicium. Once all the other parameters required
for the indicium are assembled, the indicium bitmap is generated
and printed by the client software in accordance to the
25 transmitted information.

30 FIG. 2 shows a simplified system block diagram of a typical
Internet client/server environment used by an on-line postage
system in one embodiment of the present invention. PCs 220a-220n
used by the postage purchasers are connected to the Internet 221
through the communication links 233a-233n. Preferably, these
communication links are secure. Each PC has access to one or
more printers 235. Optionally, as is well understood in the art,
a local network 234 may serve as the connection between some of
35 the PCs, such as the PC 220a and the Internet 221 or other

1 connections. Servers 222a-222m are also connected to the
Internet 221 through respective communication links. Servers
222a-222m include information and databases accessible by PCs
5 220a-220n. The on-line postage system of the present invention
resides on one or more of Servers 222a-222m.

10 In this embodiment, each client system 220a-220m includes
a CPU 223, a keyboard 224, a mouse 225, a mass storage device
231, main computer memory 227, video memory 228, a communication
interface 232a, and an input/output device 226 coupled and
interacting via a communication bus. The data and images to be
15 displayed on the monitor 230 are transferred first from the video
memory 228 to the video amplifier 229 and then to the monitor
230. The communication interface 232a communicates with the
servers 222a-222m via a network link 233a. The network link
connects the client system to a local network 234. The local
network 234 communicates with the Internet 221.

20 A client, preferably licensed by the USPS and registered
with an IBIP vendor (such as Stamps.com), sends a request for
authorization to print a desired amount of postage. The server
system verifies that the client's account holds sufficient funds
to cover the requested amount of postage, and if so, grants the
request. The server system then sends authorization to the
client system. The client system then sends image information
25 for printing of a postal indicium for the granted amount to a
printer so that the postal indicium is printed on an envelope or
label.

30 Generation and verification of the indicium is carried out
with a digital signature preferably using a Digital Signature
Algorithm (DSA) as specified in the Digital Signature Standard
(DSS) published as Federal Information Processing Standards
Publication (FIPS PUB) 186 by the U.S. Department of
Commerce/National Institute of Standards and Technology. The
following steps describe the process of creation and verification
35 of the indicium using a digital signature.

1 FIG. 3 is a data flow diagram illustrating how a VBI is
generated and verified using a digital signature. An indicium
generator, such as the previously described postage metering
server system, receives relevant information 236 from a user.
5 A subset of the relevant information is processed using a secure
hash algorithm 238 to produce a message digest 240. The message
digest is combined with a private key 242 to generate 244 a
digital signature 245.

10 The subset of the relevant information is used to generate
a 2-D barcode 248 to be printed along with a textual
representation 246 of the digital signature. The combination of
the subset of relevant information encoded as the 2-D barcode and
the textual representation of the digital signature create a VBI
15 250 that may be printed and redeemed for goods or services by the
user.

20 Redemption of the VBI requires verification of the VBI. The
subset of relevant information is read 253 from the VBI 2-D
barcode and processed 254 using a secure hash algorithm and a
message digest is created 256. The digital signature is read 258
from the VBI and combined with the message digest and a public
key 264 using a digital signal verification process 262. The
digital signature process produces a binary output. Either the
VBI is valid 266 or the VBI is invalid 268.

25 The use of a 2-D barcode and a textual representation for
printing the subset of relevant information used to create the
VBI and the resultant digital signature respectively is an
exemplary embodiment of a VBI. Other methods of combining the
subset of relevant information and the digital signature may be
used to create the VBI. For example, both the subset of relevant
30 information and the digital signature may be printed using a 2-D
barcode or both may be printed using a textual representation.
Furthermore, other methods of encoding the subset of relevant
information and the resultant digital signature may be employed
35 besides the exemplary textual and 2-D barcode encoding.

1 In one embodiment, an indicium generator hashes user
information to create a message digest and generates a digital
signature using the message digest. The above described PSD is
5 an exemplary indicium generator useful for generating postal
indicia. The PSD takes relevant information, such as the
exemplary relevant postal information in the relevant information
table 216 of FIG. 4, including postage 202, descending register
204, ascending register 206, PSD serial number 208, date of
10 mailing 210, and the like, and runs a one-way hashing algorithm
on a subset of the relevant information.

FIG. 5 depicts a hash table 510 comprising a subset of the
relevant information as depicted in the relevant information
table 216 of FIG. 4. Hashing the subset of relevant information
yields a number, called a "message digest," based on the Secure
15 Hash Algorithm (SHA-I), as specified in the Secure Hash Standard
FIPS PUB 180. A one-way hashing algorithm is a one-way
transformation that takes an input m and returns a fixed-size
output string.

20 The PSD then uses the output of the hashing algorithm (first
message digest) in conjunction with a private key to digitally
sign a digital signature using DSA. It is generally impossible
to retrieve the original message from the digitally signed
message digest. DSA is a separate algorithm for digital
25 signatures that cannot be used for encryption. Digital
signatures are used to detect unauthorized modifications to data
and to authenticate the identity of the signatory. A digital
signature is represented in a computer as a string of binary
digits. A digital signature is computed using a set of rules and
30 a set of parameters such that the identity of the signatory and
integrity of data can be verified. Signature generation makes
use of a private key to generate a digital signature. Signature
verification makes use of a public key which corresponds to, but
is not the same as, the private key. Each user possesses a
35 private key and public key pair. Private keys are never shared.

1 Anyone can verify the signature of a user by employing that
user's public key. The DSA authenticates the integrity of the
signed data and the integrity of the signatory without encrypting
5 the data, and without allowing the user to reconstruct the
underlying data used to provide the digital signature. In this
regard, the digital signature may be viewed as somewhat analogous
to a human fingerprint that accurately identifies an individual
but does not reveal the characteristics (e.g., height, weight,
10 eye color) of the individual.

Referring again to FIG. 4, the PSD then places the digital
signature in the "digital signature" field 200 of the relevant
information table 216. Next, the client software takes in
information in the relevant information table and places it in
a barcode format according to different embodiments described
15 below, and transfers the information to the user computer. The
indiciu including the digital signature and the information in
the hash table 510 of FIG. 5 is then printed on a mail piece.

The verification of the digital signature is typically
performed by the Postal service according to the following steps.
The Postal Service scans the indicium printed on the mail piece
including the digital signature with a barcode reader. The Post
Office then reads the information in the table depicted in FIG.
20 3 printed as part of the non-digitally signed portion of the
indiciu from the mail piece and then Post Office runs an
identical SHA-1 hashing algorithm on that information resulting
in a second message digest.

The DSA verification process uses the second message digest,
the scanned digital signature and the public key to verify the
identity of the sender and that the data signed by the sender has
not been changed. Note that there is no decryption involved in
this process, and no comparison between decrypted information and
human readable recipient address information appearing on the
mail piece.

1 The process of signing a digital signature and verifying it
is described in detail in FIPS PUB 186 entitled: "Digital
Signature Standard" by U.S. Department of Commerce/National
Institute of Standards and Technology.

5 As shown in the relevant information table of FIG. 4, in one
embodiment of the present invention, the Destination Delivery
Point (DDP) field 212 has a "0" value and therefore practically
eliminating the DDP field in the table. In another embodiment,
10 the DDP field is not included in the hash table 510 of FIG. 5.
Therefore, the DDP is not part of the secure hash algorithm
inputs of the hash table for generating the message digest, which
is later digitally signed.

15 In yet another embodiment, a "0" value is placed in the DDP
field of the table of FIG. 4 and the DDP value is moved to the
first five bytes of the Reserve Field 214. The resultant
relevant information table 600 is shown in FIG. 6. In this
embodiment, the hash table 510 of FIG. 5 is implemented without
including the DDP value. This embodiment also prevents the DDP
20 from being incorporated in the hash message digest. The above
three embodiments of the present invention may be combined in one
or more combination embodiments.

25 In one embodiment, the digital signature 500 is created in
plain text with an OCR-A (size I) standard and is placed to the
left of the 2D barcode 502, as shown in FIG. 7A. In this
embodiment, existing USPS scanning equipment can be used. The
OCR-A standard has been adopted for Federal Government use, and
it has been processed and approved for submittal to ANSI by the
American National Standards Committee on Information Processing,
30 X3. This standard provides the description, scope, and
identification for a set of graphic shapes to be used in the
application of optical character recognition (OCR) systems. This
style is designated OCR-A and is comprised of 96 printing
characters plus the Character Space, and includes digits,
35 letters, small letters, and special symbols. OCR-A was designed

1 to provide maximum machine efficiency under a wide range of
applications. Three sizes of graphic shapes are provided - I,
III, and IV (II is reserved for certain international
5 applications). In addition to graphic shapes and related
information, the standard provides basic requirements related to
character positioning and the ASCII code table.

In another embodiment of the present invention, the digital
signature 504 is created in plain text with an OCR-A (size I)
10 standard and is placed below the 2D barcode 506, as shown in FIG.
7B. In this embodiment, existing USPS scanning equipment can be
used. In yet another embodiment of the present invention, the
digital signature 508 is created in plain text with a smaller
size OCR-A standard and is placed below the 2D barcode 510, as
15 shown in FIG. 7C.

The above described VBI generation and verification process
is useful in a variety of applications. For example, the VBI
generation and verification process can be used in on-line
systems to issue postage, tickets, currency, vouchers, coupons
and traveler's checks. An exemplary on-line postage system is
20 described in U.S. patent Application No. 09/163,993 filed
September 29, 1998, the contents of which are hereby incorporated
by reference. The on-line postage system includes an
authentication protocol that operates in conjunction with the
USPS. The system utilizes on-line postage system software
25 comprising user code that resides on a client system and
controller code that resides on a server system. The on-line
postage system allows a client to print a postal indicium at
home, at the office, or any other desired place in a secure,
convenient, inexpensive and fraud-free manner. The system
30 comprises a user system electronically connected to a server
system, which in turn is connected to a USPS system.

In one embodiment, the server system is remotely located in
a separate location from the client. All communications between
35 the client and the server are preferably accomplished via the

1 Internet. Referring again to FIG. 1, a remote client system 220a
connected to a server system 180 via the Internet 221. The
client system includes a processor unit 223, a monitor 230,
5 printer port 106, a mouse 225, a printer 235, and a keyboard 224.
Server system 180 includes Postage servers 132, Database 130, and
cryptographic modules 134.

10 The Server system 180 is designed in such a way that all of
the business transactions are processed in the servers and not
in the database. By locating the transaction processing in the
servers, increases in the number of transactions can be easily
handled by adding additional servers. Also, each transaction
processed in the servers is stateless, meaning the application
does not remember the specific hardware device the last
15 transaction utilized. Because of this stateless transaction
design, multiple machines can be added to each subsystem in order
to handle increased loads. In one embodiment, load balancing
hardware and software techniques are used to distribute traffic
among the multiple servers.

20 Furthermore, each cryptographic module is a stateless
device, meaning that a PSD package can be passed to any device
because the application does not rely upon any information about
what occurred with the previous PSD package. A PSD package for
each cryptographic module includes all data needed to restore the
25 PSD to its last known state when it is next loaded into a
cryptographic module. This includes the items that the IBIP
specifications require to be stored inside the PSD, information
required to return the PSD to a valid state when the record is
reloaded from the database, and data needed for record security
30 and administrative purposes.

35 In one embodiment, the items included in a PSD package
include ascending and descending registers, device ID, indicium
key certificate serial number, licensing ZIP code, key token for
the indicium signing key, the user secrets, key for encrypting
user secrets, data and time of last transaction, the last

1 challenge received from the client, the operational state of the PSD, expiration dates for keys, the passphrase repetition list and the like.

5 As a result, the need for specific PSDs being attached to specific cryptographic modules is eliminated. A Postal Server subsystem provides cryptographic module management services that allow multiple cryptographic modules to exist and function on one server, so additional cryptographic modules can easily be
10 installed on a server. This Postal Sever subsystem is easy to scale by adding more cryptographic modules and using commonly known Internet load-balancing techniques to route inbound requests to the new cryptographic modules.

15 Postage servers 132 provide indicium creation, account maintenance, and revenue protection functionality for the on-line postage system. The Postage servers 132 include several physical servers in several distinct logical groupings, or services as described below. The individual servers could be located within one facility, or in several facilities, physically separated by
20 great distance but connected by secure communication links.

25 Cryptographic modules 134 are responsible for creating PSD packages and manipulating PSD package data to protect sensitive information from disclosure, generating the cryptographic components of the digital indicium, and securely adjusting the user registers. When a user wishes to print postage or purchase additional postage value, a user state is instantiated in the PSD implemented within one of the cryptographic modules 134. Database 130 includes all the data accessible on-line for
30 indicium creation, account maintenance, and revenue protection processes. Postage servers 132, Database 130, and cryptographic modules 134 are maintained in a physically secured environment, such as a vault.

35 In one embodiment, as illustrated in FIG. 8, the Postal Server subsystem 41 is physically comprised of at least one cryptographic module 52, at least one Postal Server 53 and at

1 least one PostalX Server (PSX) 54. When the workload is increased, the number of each of these devices can be increased to accommodate the additional work.

5 In one embodiment of the present invention, the cryptographic modules 52 are FIPS 140-1 certified hardware cards or other hardware that include firmware to implement PSD functionality in a cryptographically secure way. The cryptographic modules are inserted into any of the servers in the Postal Server Infrastructure. The cryptographic modules are responsible for creating PSDs and manipulating PSD data to generate and verify digitally signed indicia. Since the PSD data is created and signed by a private key known only to the card, the PSD data may be stored externally to the cryptographic modules without compromising security.

10 In one embodiment of the present invention, Postal Server 53 is a standalone server process that provides secure connections to both the clients and the server administration utilities, providing both client authentication and connection management functionality to the system. Postal Server 53 also houses postal-specific services that require high levels of security, such as purchasing postage or printing indicia. Postal Server 53 is comprised of at least one server, and the number of servers increases when more clients need to be authenticated, are purchasing postage or are printing postage indicia.

25 In one embodiment of the present invention, PXS 54 is a standalone server process that provides trusted plain-text access to in-vault components. PXS 54 hosts postal-specific services that are protected from access external to the vault via a firewall. The PostalX Services provide business logic for postal functions such as device authorization and postage purchase/register manipulation. The PXS services require cryptographic modules to perform all functions because the PXS services are vital to the system's integrity and are protected by encryption. The PXS services can be located on one physical

1 server or multiple machines depending on the number of postal-specific transactions.

5 When a client system sends a postage print request to the server system, the request must be authenticated before the client system is allowed to print the postage, and while the postage is being printed. The client system sends a password (or passphrase) entered by a user to the server system for verification. If the password fails, a preferably asynchronous dynamic password verification method terminates the session and printing of postage is aborted. Also, the server system communicates with a system located at the USPS for verification and authentication purposes. The information processing components of the on-line postage system include a client system, a postage server system located in a highly secure facility, a USPS system and the Internet as the communication medium among those systems. The information processing equipment communicates over a secured communication line.

15 The on-line postage system does not require any special purpose hardware for the client or user system. The client system is implemented in the form of software that can be executed on a user computer (client system) allowing the user computer to function as a virtual postage meter. The software can only be executed for the purpose of printing the postage indicium when the user computer is in communication with a server computer located, for example, at a postage meter vendor's facility (server system). The server system is capable of communicating with one or more client systems simultaneously.

25 The above described VBI generation and verification process can be used in on-line systems to issue tickets. In one embodiment, an indicium generator is used to provide tickets for air travel. Functionally, the system may be broken down into two parts, itinerary generation and Passenger Validation Information (PVI).

1 The exemplary ticketing system includes the purchase and
printout of a ticket, such as an airline itinerary with an
associated indicium that contains PVI used for boarding purposes.
5 An airline ticket is used as an example throughout this example,
however, it is understood that the ticketing system of the
present invention is not limited to printing airline tickets. The
ticketing system is capable of printing all types of tickets and
value-bearing items such as, tickets for entertainment events,
10 coupons, checks, gift certificates, and the like.

15 In the exemplary case of airline tickets, PVI includes
fields such as ticket number, passenger name, seat number, flight
number, etc. The user experience happens in the context of a
standard web browser. A web site is provided that allows a user
to purchase an airline ticket. After purchasing the ticket, the
user is presented with an itinerary with an image of an indicium
that contains the PVI associated with that ticket. The user is
able to print out the web page using the standard print
functionality provided by the browser.

20 The second part of the system includes the user interaction
at the boarding gate. A standalone boarding application that
interfaces with a scanner, for example, a Metanetics IR2000
scanner is presented. The printed page is scanned using the
scanner, and the application displays the relevant PVI embedded
25 in the indicium. Additionally, on a first time scan of the
indiciu, the application indicates that the passenger is cleared
for boarding. Subsequent scans of the same indicium shows that
the boarding pass has already been used. A scan of an indicium
NOT generated by the system presents a "not valid indicium"
30 message to the user indicating that the scanned indicium is not
in the inventory database.

35 The following section describes the design and data flow to
implement the functional requirements of one embodiment the
system. This design eliminates the need for the system to host

1 an application to generate indicia directly onto the web server data store. This minimizes coding and deployment efforts.

5 FIG. 9 is deployment diagram of an exemplary ticketing system according to one embodiment of the present invention. An indicium generator 706 is operably coupled to a membership database 710. The indicium generator server generates indicia and stores them in the membership database for tracking during a redemption process.

10 The indicium generator is operably coupled via the Internet 221 to a distributor Web server 700. The distributor Web server provides a user interface in the form of a Web site for the purchase of tickets. The distributor Web server also supplies the business rules controlling the purchase of tickets by a user. A Web browser running on an end-user's machine 707 is operably
15 coupled to the distributor Web server via the Internet. A user uses the Web site hosted by the distributor Web server to purchase a ticket that is printed on a printer device 902.

20 A scanning machine 800 is operably coupled to a scanning device 900 for scanning tickets and operably coupled to the indicium generator server via the Internet. The scanning machine scans the ticket and contacts the indicium generator server to determine that the scanned ticket is valid.

25 FIG. 10 is a diagram illustrating the data flow between a ticket distributor web server and an indicium generator system to implement itinerary generation function.

A web server 700 hosts a web site that allows a user to navigate and purchase 702 a ticket. The web server is responsible for the Look and Feel (L&F) of the web site.

30 The web server, after application processing logic relevant to ticket reservation and generation, may generate a web page 704 with itinerary information, marketing data, and link to the indicium graphic. The link references an indicium generator web server 706 with sufficient parameters (PVI plus any other
35

1 relevant reference data) in order to later generate the associated indicium image.

5 A browser hosted by end user machine 707 then displays the resultant page, resolving 708 the indicium link with the indicium generator server.

10 Upon receiving the request for the indicium image, the indicium generator web server enters the associated PVI data and other relevant data into the Indicium generator database 710 for later reference. After storing the data, the server generates the indicium image based on the PVI data.

The indicium image is returned 712 back to the browser for display within the itinerary page. At this point the user may print the page.

15 FIG. 11 is a diagram illustrating the data flow between the ticket distributor and indicium generator systems to implement PVI validation function.

20 A scanning computer 800 hosts an application that interfaces with a scanner, such as a Metanetics IR2000 scanner. The application is responsible for providing a user interface to display the PVI data. Upon scanning the indicium, the PVI data from the indicium is extracted, and forwarded 802 to an indicium generator server 706 for processing.

25 Upon receiving the request, the indicium generator server application logic validates 804 the indicium data for referential integrity and existence within an indicium generator database 710. If the indicium has not already been used, it is marked as used.

30 If the PVI is being used for the first time, the indicium generator server sends a command 806 to the ticket distributor server to indicate the associated passenger has boarded the plane.

35 The indicium generator server returns a result 808 back to the scanning application indicating one of three possible events: valid PVI, PVI already used; or invalid PVI data. The scan

1 utility displays the contents of the indicium and the server
result.

5 It will be recognized by those skilled in the art that
various modifications may be made to the illustrated and other
embodiments of the invention described above, without departing
from the broad inventive scope thereof. It will be understood
therefore that the invention is not limited to the particular
embodiments or arrangements disclosed, but is rather intended to
10 cover any changes, adaptations or modifications which are within
the scope and spirit of the invention.